341 = (21-10) (21+10)

الع مع ما ان 2 ادلي مع ١١

2 = 1 (mod 11)

مِعنعُ

 $\frac{31}{2} = (2^{10})^3 \cdot 2 = 2 \pmod{1}$ 

عنال ترونه

 $2^{"} \equiv (2^{5})^{2} 2 \pmod{31}$   $2^{"} \equiv (32)^{2}, 2 \pmod{31}$   $\equiv (1)^{2}, 2 \pmod{31}$   $2^{"} \equiv 2 \pmod{31}$ 

حبه لمانه لسبق

31.11 = 2 (mod 31.11)

341 2 = 2 (mod 341)

2.2 = 2 (mod 341)

عان 2 أولى مع كفاس أي 2 أولى مع ١٩١ ومات ي كلي الافتهار من طرفي

340 2 = 1 (mod 341)

( كان 2 و ١١ أوليا برهينا بينها

2 = 1(mod11) (210)34 = 1 (mod11)

340 2 = 1 (mod 11)

- 多 موزاييك

⇒ 11] (2 -1)

صناعبة ثانية عبان و الازوليار عيما سِنها

30 2 = 1 (mod 31)

 $\frac{340}{2} = (2)^{11} \cdot 2^{10} = 2^{10} \pmod{31}$  $= (2^{5})^{2} \pmod{31} = 1 \pmod{31}$ 

 $\frac{3^{40}}{2} = 1 \pmod{31}$ =) 31 |  $(2^{3^{40}} - 1)$ 

علان ١١ و ١١ وأوليام عنوا سنرا مالكاني بأم ما (2 ما) ما ١٠١١ علان ١١ و عنوا سنرا مالكاني بأم ما عنوا ما ١١٠ (2 عنوا ما الله عنوا ما ال

340 = 1(mod 341)

عنالمثال يسين أن عكس مرجنة حزما سي صحبي في اكالة لعامة

2 = 1(mod 341)

یا 34۱ سے آولیاً \* ای اذاکین

q = 1(modm)

وبالآك اسم بالعنزورة ان يكوم ساولياً

2-0 h) = D

\* الأعداد هذه المنوع . 2 = 2 (modn) = 2 . مستى ا مثاه أولية وهي محموكة عير هنتريس

رنی ا حوال اهم ای موال اهم ای اور کرده اهم اور کرده ای اور کرده ا

a = 1 (mod 35)

را = ا(mod 5) ع مرا = ا(mod 5) .

م = ا(mod 5) ع مرا = ا(mod 5) .

م = ا(mod 5) ع مرا = ا(mod 5) .

الا = الاسم عنوابيع وباللا وباللا وبالله عنوابيع وبالله وبالله عنوابيع وبالله عنوابيع وبالله عنوابيع وبالله عنوابيع وبالله و

 $(a-b) \equiv 0 \pmod{168}$   $(8-b) \equiv 0 \pmod{168}$  168 = 3.7.8 42 = 2.3.7

q(a,p,qz)=1

هناسینیان ۵ مع 3 ، : و ۲ م 8 ۱=(8 و م) 6 = (4, م) 6 = (3 و م) 6 ا=(8 و م) 6 = (4 و م) 6 = (3 و م) 6

 $a^2 \equiv 1 \pmod{3}$   $a^6 \equiv 1 \pmod{3}$ 

ومالثالي لانكبت

(8 ف ما) ا= أه فان 8 لاست عد أولى ولاتبنطق

多まで

عليا مرهمة حرفا.

ا=(8,010) ملاه لاعکن ان یکو نا روجیس عودی والا حزی روجی و الا حزی والا حزی روجی و دی و الا حزی از دی دوجی و دیات کے دو اس حزدیا م

 $0^{2} \equiv 1 \pmod{8}$   $0^{2} \equiv 1 \pmod{8}$   $0^{3} \equiv 1 \pmod{8}$   $0^{4} \equiv 1 \pmod{8}$   $0^{5} \equiv 1 \pmod{8}$   $0^{6} \equiv 1 \pmod{8}$ 

وباساك جلاد 3.7.3 ستم (6° - 6°)

\* جبهدة ومليت ساست المهشم: اذاكان Pعددة أوليا والم  $(P-1)! \equiv -1 \pmod{P}$   $m_{P} \mid (P-1) + [T] = 0$  (-1) = P-1  $(P-1)! \equiv (P-1) \pmod{P}$   $(P-1)! \equiv (P-1) \pmod{P}$ 

1 /

(P-1)(P-2)! = (P-1) (mod P)
عِمل الموتفيا ولك عاتب المحل المعلى على (P-1) (المحل على العب علي المعلى عليه عائن الم

(P-2)! = 1(modp)

sapar el color de

()如()如

1 1

1 = -1 (mod 3) 2 = -1 (mod 3) الرهان المنعا 2:4 همقت الرهان المنعا 1:4 همقت المنعا 1:4 محمد المنعادة 1:4 محمد المنعودة الم

A= + Zp180, +T8

A={2,3,---, P-2} ا مبتة المعرية الما رتبة المعرية

عان م آولي وبالتاك طرهه من و عوعد روجي

ره کو (1) کو (1) م

لعة هَنَّا عِنَا لِهُ اللَّهِ

P=13 A=5 2.3, 4,5,6,7,8,9,10,117 4(10) =1 (mod(3)

عند تتوزع م اک (  $\frac{P-3}{2}$ ) زوع جیت ماجل جزب آی روجین میرافقین میرافی میرافی میرافی میرافی میرافین می

2.3. -- (P-2) = 1 (mod P)

يعذ والمرابي انتطابق

2.3. -- (P-2)(P-1) = (P-1)(modP)  $(P-1)! = -1 \pmod{P}$ 

一多 春一年

اواكان 2 رم اواكان 2 رم وعدائد 1 مكوم أوكي الرهام

(n-1)! = -1 (modn)

1 /

مناحية أحزى :

n | (n-1)!+1 الموهن العزبين ا+!(1-n) | n | (2) \_\_\_ (2) من العلامتين (1) و(2)

ا= 2!(۱-۱0)- ۱+!(۱/-۱0) كل مهاتك ا= له اوارار (۱۱/-۱۵) كل مهاتك ا= له وهنا شاوعت مع كلم ١١ لسب أولياً ومانتك م الكلي ١١ أولياً ومانتك م الكلي ١٠ أولي .

Elipus

=

E

E

E

5

=

وكين هييائة فبرهنة والمسن وى حاكل المنو الآفي المنو المرق المرق

ورك في المعيار للأعداد الأولي سبب مرىة ترايد الا وهاجة عنو بكوم n عدد كير 7

> سرون ا ا ست آن

 $18! = -1 \pmod{437}$   $(20)^{2} < 437 < (21)^{2}$   $(21)^{2} - 437 = 4$   $437 = 19 \cdot 23$ 

舎まご言の

```
البُّ إِنْ لَعَدُدُ
         127 [7.(1261) + 51]
         (1261 = -1 (modist)
        126 (125) = -1 (modist)
      (-1) (116) = -(modest)
        (126): = 1 (mad 127)
      7.(125)! = 7 (modiz +)
                                        المستعملية الم
  5! + T(125); = 7+5; (mad(27)
              = 127 (mod 12.7)
51,+7.(115)! = a (mod 117)
     127 [7 (126)] +5: ]
العام الكر وللمعات على عبرها وعاهدة وعا وعاهدة وعدي ولعطمة إلمادية
                  اذاكف المحددة أولية الروية عدم المدال النطابع
       x1 = -1 (mod P)
                                      وفاحصها ووكات
           P = 1 (mod4)
                                  واجامه الحداث اختكان
               P = 1(mad4)
                                                   جا ن
carbindo x = ( P-1 )!
```

南京皇

x2 = -1(madp)

1111

 $x = (\frac{5-1}{2})$ ; = 2! = 2

(2)1 = 4 = -1(mobs)

 $x = (\frac{13-1}{2})^{\frac{1}{2}} = 6! = 720$ 

(770) = (modB)

much sindichan